Amended Claim 10 is now directed to a data processing system having various processing means. Thus, the § 101 rejection is believed to be overcome.

Rejection under 35 U.S.C. § 112

Claim 10 was rejected under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements. Applicants respectfully traverse such rejection insofar as it might apply to the claims as amended herein.

Claim 10 has been amended to include essential structural cooperative relationships of elements. Thus, the § 112 rejection is believed to be overcome.

Rejection under 35 U.S.C. § 102

Claims 1-4 and 10-13 were rejected under 35 U.S.C. § 102(b) as being anticipated by *Spies et al.* (US 5,689,565). Applicants respectfully traverse such rejection insofar as it might apply to the claims as amended herein.

Amended Claim 1 (and similarly Claim 10) now recites a step of "in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key" (lines 5-6), a step of "storing said encrypted cookie in a non-protected storage device within said data processing system" (lines 7-8), a step of "in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key" (lines 9-11), and a step of "sending said decrypted cookie to said browser program" (line 12). Thus, according to the claimed invention, a cookie generated by an application from a remote server is encrypted by a public key of a public-private key pair before the cookie is stored in a non-protected storage device. When the encrypted cookie is being requested by a browser program, the encrypted cookie is then decrypted by a private key of the public-private key pair before sending to the browser program. As such, a cookie can be securely stored in a non-protected storage device of a data processing system.

Generally, since *Spies* is not related to Internet applications, thus *Spies* does not disclose the usage of cookies or browser programs within a data processing system, as claimed.

Specifically, *Spies* does not teach or suggest the claimed step of encrypting a cookie by a public key of a public-private key pair before the cookie is stored in a non-protected storage device within a data processing system. In addition, *Spies* does not teach or suggest the claimed step of decrypting the encrypted cookie by a private key of the public-private key pair before sending the cookie to the browser program. Because the claimed invention includes novel features that are not taught or suggested by *Spies*, the § 102 rejection is believed to be overcome.

CONCLUSION

Claims 1-7 and 10-16 are currently pending in the present application. For the reasons stated above, Applicants believe that independent Claims 1 and 10 along with their respective dependent claims are in condition for allowance. The remaining prior art cited by the Examiner but not relied upon has been reviewed and is not believed to show or suggest the claimed invention.

No fee or extension of time is believed to be necessary; however, in the event that any fee or extension of time is required for the prosecution of this application, please charge it against Deposit Account No. **50-0563**.

Respectfully submitted,

Antony P. Ng
Registration No. 43,427
BRACEWELL & PATTERSON, LLP
P.O. Box 969
Austin, Texas 78767-0969
(512) 472-7800

ATTORNEY FOR APPLICANTS

<u>**REDACTED CLAIMS**</u>

1.   (Amended) A method [in a data processing system for maintaining a secure data block within said] <u>for protecting security of a cookie stored within a data processing</u> system, said method comprising [the steps of]:

        [establishing a block of data within said system, said block of data being associated with a particular user and a particular application;]

        [establishing] <u>storing</u> a [hardware master] <u>encryption</u> key pair [for said system, said hardware master key pair including a master] <u>having a</u> private key and a [master] public key <u>in a protected storage device within said data processing system;</u>[, said hardware master key pair being associated with said system so that said master private key is known to only said system; and]

        <u>in response to the receipt of a cookie generated by an application from a remote server,</u> encrypting <u>said cookie with</u> said [block of data utilizing said master] public key<u>;</u>[, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of decrypting said encrypted block of data.]

        <u>storing said encrypted cookie in a non-protected storage device within said data processing system;</u>

        <u>in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key; and</u>

        <u>sending said decrypted cookie to said browser program.</u>

2.   (Amended) The method according to claim 1, [further comprising the step of storing said encrypted block of data in a] <u>wherein said</u> non-protected storage device <u>is a hard drive.</u>

3.   (Amended) The method according to claim [2] <u>1</u>, further comprising [the steps of:

        establishing] <u>providing</u> an encryption device having an encryption engine and <u>said</u> protected storage device[, said protected storage device being] accessible only through said encryption engine[; and

        storing said hardware master key pair in said protected storage device].

4.   (Amended) The method according to claim 3, <u>wherein said encrypting</u> further [comprising the step of said encryption engine] <u>include</u> encrypting said [block of data] <u>cookie</u> utilizing said [master public key stored in said protected storage] <u>encryption</u> device.

5.   (Amended) The method according to claim 4, <u>wherein said decrypting</u> further [comprising the step of a remote data processing system executing said application] <u>includes decrypting said encrypted cookie utilizing said encryption device</u>.

6.   (Amended) The method according to claim 5, <u>wherein said sending</u> further [comprising the step of establishing a browser program for accessing said application] <u>includes transmitting said decrypted cookie from said encryption device to said browser program</u>.

7.   (Amended) The method according to claim 6, further comprising <u>transmitting said decrypted cookie from said browser program to an application executing in a remote server</u> [the steps of:

        said browser program initiating a session with said application;

        said browser requesting said encryption device to decrypt said encrypted block of data;

        in response to said request, said encryption device decrypting said encrypted block of data utilizing said master private key; and

        said encryption device transmitting said decrypted block of data to said browser program].

8.   cancelled

9.   cancelled

10.   (Amended) A data processing system [for maintaining a secure data block] <u>capable of protecting the security of a cookie stored</u> within said <u>data processing</u> system, <u>said data processing</u> comprising:

        <u>a protected storage device for storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system;</u>

        <u>means for utilizing said public key to encrypt said cookie, in response to the receipt of a cookie generated by an application from a remote server;</u>

        <u>a non-protected storage device within said data processing system for storing encrypted cookie;</u>

        <u>means for utilizing said private key to decrypt said encrypted cookie, in response to an access request for said encrypted cookie by a browser program executing within said data processing system; and</u>

        <u>means for sending said decrypted cookie to said browser program.</u>

        [said system executing code for establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

said system executing code for establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system; and

said system executing code for encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of decrypting said encrypted block of data.]

11. (Amended) The data processing system according to claim 10, wherein said non-protected storage device is a hard drive [further comprising said system executing code for storing said encrypted block of data in a non-protected storage device].

12. (Amended) The data processing system according to claim [11] 10, further comprising[:]

an encryption device having an encryption engine and said protected storage device[, said protected storage device being] accessible only through said encryption engine[; and

said encryption device executing code for storing said hardware master key pair in said protected storage device].

13. (Amended) The data processing system according to claim 12, wherein said means for utilizing said public key to encrypt said cookie is [further comprising] said encryption engine [executing code for encrypting said block of data utilizing said master public key stored in said protected storage device].

14. (Amended) The data processing system according to claim 13, wherein said means for utilizing said private key to decrypt said encrypted cookie is said encryption device [further comprising a remote data processing system capable of executing said application].

15. (Amended) The data processing system according to claim 14, wherein said sending means further includes means for transmitting said decrypted cookie from said encryption device to said browser program [further comprising said system executing code for establishing a browser program for accessing said application].

16. (Amended) The data processing system according to claim 15, further comprising means for transmitting said decrypted cookie from said browser program to an application executing in a remote server [:

said system executing code for said browser program initiating a session with said application;

said system executing code for said browser requesting said encryption device to decrypt said encrypted block of data;

in response to said request, said encryption device capable of decrypting said encrypted block of data utilizing said master private key; and

said encryption device executing code for transmitting said decrypted block of data to said browser program].

17.   cancelled
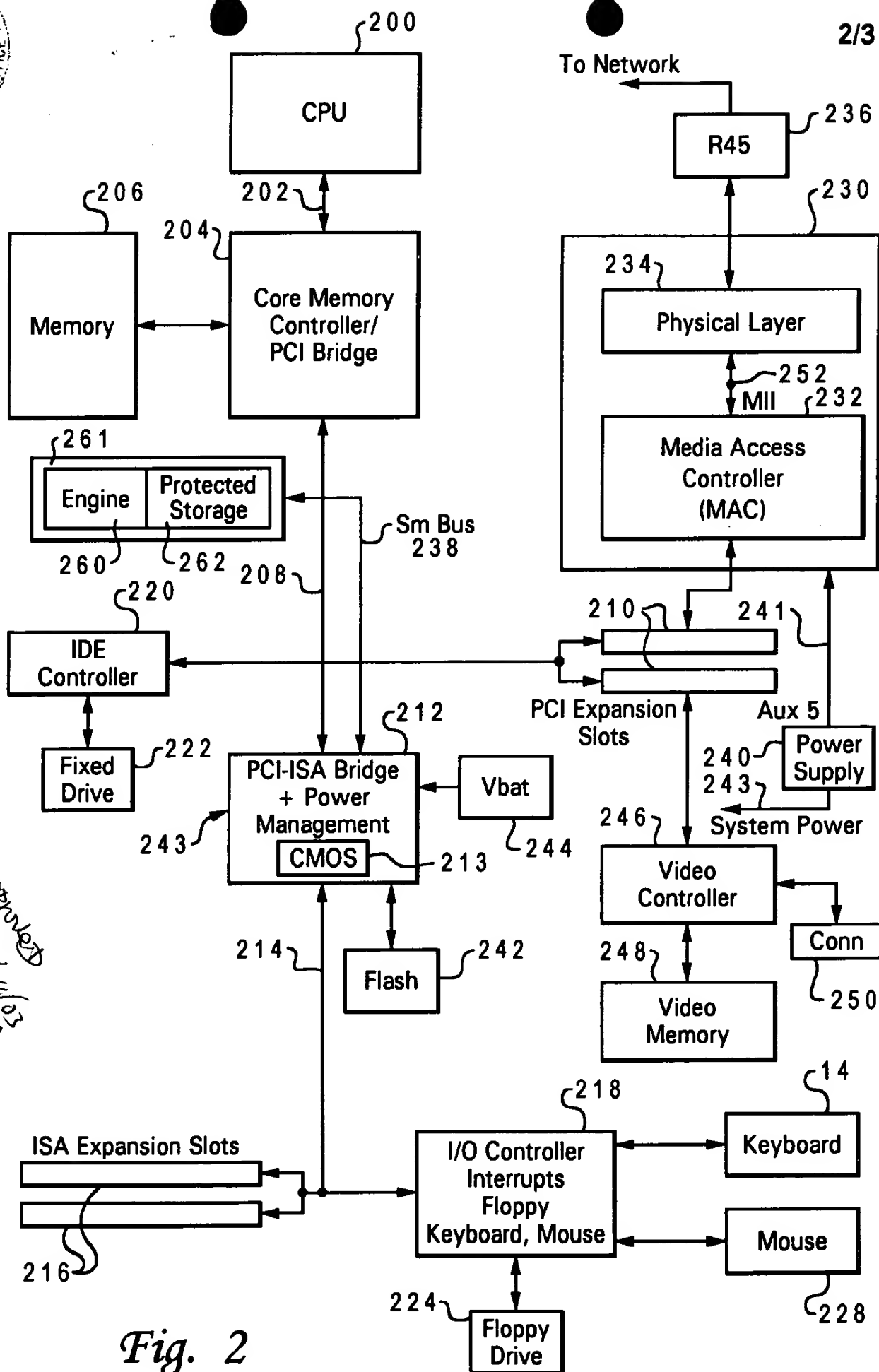
18.   cancelled

19.   cancelled

To Network

R45 236

Physical Layer 234

MII 252

Media Access Controller (MAC) 232

230

CPU 200

202

Core Memory Controller/ PCI Bridge 204

Memory 206

261
Engine | Protected Storage
260 262 208

Sm Bus 238

IDE Controller 220

Fixed Drive 222

PCI Expansion Slots 210 241

Aux 5

PCI-ISA Bridge + Power Management 212

CMOS 213

Vbat 244

243

214

Flash 242

ISA Expansion Slots

216

Power Supply 240

System Power 243

Video Controller 246

Conn 250

Video Memory 248

I/O Controller Interrupts Floppy Keyboard, Mouse 218

Keyboard 14

Mouse 228

Floppy Drive 224

Fig. 2